(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
3 juin 2004 (03.06.2004)

PCT

(10) Numéro de publication internationale
WO 2004/046017 A2

(51) Classification internationale des brevets[7] : B81B 1/00

(21) Numéro de la demande internationale :
PCT/FR2003/050119

(22) Date de dépôt international :
13 novembre 2003 (13.11.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
02 14281 15 novembre 2002 (15.11.2002) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **GEMPLUS** [FR/FR]; Avenue du Pic de Bertagne, Parc d'activités de GEMENOS, F-13420 GEMENOS (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **JOYE, Marc** [BE/FR]; 19 rue Voltaire, F-83640 SAINT ZACHARIE (FR). **VILLEGAS, Karine** [FR/FR]; 162, Chemin de Lieutaud, F-13420 GEMENOS (FR).

(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés *(régional)* : brevet ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :
— *sans rapport de recherche internationale, sera republiée dès réception de ce rapport*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(54) Title: INTEGER DIVISION METHOD WHICH IS SECURE AGAINST COVERT CHANNEL ATTACKS

(54) Titre : PROCEDE DE DIVISION ENTIERE SECURISE CONTRE LES ATTAQUES A CANAUX CACHES

(57) Abstract: The invention relates to a cryptographic method involving an integer division of type q = a div b and r = a mod b, wherein a is a number of m bits, b is a number of n bits, with n being less than or equal to m, and b_{n-1} being non-null and the most significant bit of b. In addition, each iteration of a loop subscripted by i, which varies between 1 and m-n+1, involves a partial division of a word A of n bits of number a by number b in order to obtain one bit of quotient q. According to the invention, the same operations are performed with each iteration, regardless of the value of the quotient bit obtained. In different embodiments of the invention, one of the following is also performed with each iteration: the addition and subtraction of number b to/from word A; the addition of number b or a complementary number åb of b to word A; or a complement operation at 2^n of an updated datum (b or åb) or a dummy datum (c or åc) followed by the addition of the datum updated with word A.

(57) Abrégé : L'invention concerne un procédé cryptographique au cours duquel on réalise une division entière de type q = a div b et r = a mod b, avec a un nombre de m bits, b un nombre de n bits avec n inférieur ou égal à m et b_{n-1} non nul, b_{n-1} étant le bit de poids le plus fort de b, procédé au cours duquel, à chaque itération d'une boucle indicée par I variant entre 1 et m-n+l, on réalise une division partielle d'un mot A de n bits du nombre a par le nombre b pour obtenir un bit du quotient q. Selon l'invention, les mêmes opérations sont réalisées à chaque itération, quelque soit la valeur du bit de quotient obtenu. Selon différents modes de réalisation, on réalise ainsi à chaque itération: soit une addition et une soustraction du nombre b au mot A, soit une addition du nombre b ou d'un nombre complémentaireåb de b au mot A ou soit une opération de complément à 2^n d'une données actualisée (b ouåb) ou d'une donnée fictive (c ouåc) puis une opération d'addition de la donnée actualisée avec le mot A.

WO 2004/046017 A2